
THE PATRIOT
Identity Recovery Guide

Disclaimer

The material herein is accurate to the best of the author's knowledge. However, the author's opinions may change. The reader is encouraged to verify the status of those opinions.

This publication is designed to provide accurate and authoritative information in regard to the subject matter covered. It is sold with the understanding that the publisher is not engaged in rendering legal, accounting, or other professional service. If legal advice or other expert assistance is required, the services of a competent professional person should be sought.

In no event shall Freedom Writers Publishing, Rama Marketing LLC, and/or its agents and affiliates be liable to any party for direct, indirect, special, incidental, or consequential damages of any kind whatsoever arising out of the use of the information contained herein. Freedom Writers Publishing, Rama Marketing LLC and/or its agents and affiliates specifically disclaim any guarantees, including, but not limited to, stated or implied potential profits or rates of return or investment timelines.

The information contained in this kit/book/course and its several complementary guides, is meant to serve as a comprehensive collection of time-tested and proven strategies that the author(s) have deemed successful to meet the intended results. Summaries, strategies, tips and tricks are only recommendations by the authors, and reading this kit does not guarantee that one's results will exactly mirror our own results. The authors have made all reasonable efforts to provide current and accurate information for the readers of this product. The authors will not be held liable for any unintentional consequences, errors, or omissions that may be found.

The material in this kit may include information, products, or services by third parties. Third Party materials comprise of the products and opinions expressed by their owners. As such, the authors of this guide do not assume responsibility or liability for any Third Party Material or opinions.

The publication of such Third Party materials does not constitute the authors' guarantee of any information, instruction, opinion, products or service contained within the Third Party Material. Use of recommended Third Party Material does not guarantee that your results will mirror our own. Publication of such Third Party Material is simply a recommendation and expression of the authors' own opinion of that material.

Whether because of the general evolution of the Internet, or the unforeseen changes in company policy and editorial submission guidelines, what is stated as fact at the time of this writing, may become outdated or simply inapplicable at a later date. This may apply to this product, our affiliated website platforms, as well as, the various similar companies that we have referenced in this kit, and our several complementary guides. Great effort has been exerted to safeguard the accuracy of this writing. Opinions regarding similar website platforms have been formulated as a result of both personal experience, as well as the well documented experiences of others.

TABLE OF CONTENTS

INTRODUCTION

The day begins just like any other one normally would. You're on your way to work in the morning and realize you need to make a quick pit stop at the gas station before you run out of fuel completely. You fill up the tank and grab a coffee and newspaper once inside the store. You offer the cashier your credit card and are stunned when she tells you that it has been rejected. As the wave of embarrassment rushes over you, you fumble around in your pockets for enough cash to cover the entire bill. On the way out you stop at the ATM to replace the money you had in your pocket and to your horror the screen tells you that your account has insufficient funds. Panicked now, you arrive at the office and immediately check your online credit card and bank statements. Your checking account is in overdraft which means there must be some kind of mistake as you know there was enough in there for the next mortgage payment and then some. Your credit card statement shows thousands upon thousands of dollars worth of purchases over the last two weeks that you know you didn't make. When you finally call the bank to find out what's going on they pass you over to a supervisor who tells you that the loan you recently applied for has been denied. Because you've applied for credit at a number of other places within the last month they aren't comfortable in extending a loan to you based on your current debt load.

With your head spinning and thoughts coming at you a million a minute you finally realize…you have just become the latest victim of Identity Theft.

The commercials are all over television – and they certainly are attention-grabbing! They're the ones where the heavy, bald guy is sitting in his easy chair talking in a squeaky female voice about all the clothes he bought – including a bustier. Or the little old lady speaking with the gruff voice of a younger man about the sweet motorcycle she now owned.

While we might find these commercials funny, the real victims of identity theft find them disturbing and even painful. The media uses these types of ads to alert us to the crime of identity theft and how everyday people can be affected. You don't have to have a lot of money to be taken advantage of. All you need is a social security number – which, of course, we all have.

The criminals who perpetrate the crime of identity theft are sly and cunning. Before you can even know it, you're credit is ruined and you must "jump through hoops" just to get it repaired a small bit. Identity theft is a serious crime – one that is occurring with an alarming frequency. The statistics are mindboggling.

- 1 in 4 US households have been victimized
- 10 million people last year affected
- Loss to businesses tops $47.6 billion
- Loss to victims about $5 billion
- Each victim spends about 30 hours trying to recover their name.

The problem of identity theft has become the number one fear of consumers in the world today, and unfortunately, it's becoming more and more common.

Consider the following cases of identity theft and how it can be used to perpetrate crime:

- Several people obtained names and Social Security numbers of several hundred high-ranking active-duty and retired U.S. military officers from a public Internet Website. They used the officers' names and numbers to apply for credit cards and bank and corporate credit in the officers' names.
- A man stole the identities of more than 100 people by working with a woman who had worked in the payroll department of a cellular telephone company. In that position, the woman had access to confidential employee information such as Social Security numbers and home addresses. Using the employees' names and Social Security numbers, the man was able to access their stock trading accounts at an online brokerage and transfer money to another account that he had set up. One victim had more than $287,000 taken from his brokerage account without his knowledge.
- When various people who picked up their mail at a U.S. post office threw away merchandise catalogs, which contained identifying information such as their names and account numbers, a woman went through the trash, removed the catalogs, and used the identifying information to order merchandise in other people's names.
- A man stole private bank account information about an insurance company's policyholders. He used that information to deposit approximately 4,300 counterfeit bank drafts, totaling

more than $764,000, and to withdraw funds from the accounts of the policyholders.

It can happen without you even knowing it, and can ruin lives. It can take a con just a few minutes to ruin a good name you've worked to build.

With the internet, identity theft is going global. The scary part is these criminals are getting better and better. You can become a victim and not even know it was YOU who started the cycle. It can start with a simple e-mail.

The phenomenon has sprung even more non-legitimate scams preying on the fears of having one's identity stolen. People are cashing in on the hysteria and costing consumers even more money.

The victims believe, from experience, that it is the only crime where the suspect is presumed innocent before proven guilty, and the victim is "guilty" until proven "innocent." In this book, we'll take an in-depth look at identity theft. We'll explore how your personal information can get stolen as well as ways to protect yourself. This book will tell you the steps you need to take to recover your credit and stop the thieves who stole what you yourself worked to build.

WHAT IS IDENTITY THEFT?

As the quickest growing crime in America, identity theft affects approximately 7 –10 million people every single year.
Simply put, identity theft is the act of using someone else's personal information, or their actual identity for personal gain. Frighteningly it happens without you even knowing it and once you have become aware of it, in most cases the damage has already been done.

Types of Identity Theft

Although there are many different methods that one can utilize to rip someone off in an identity theft type scam, there are really only two basic types of actual identity theft.
The first of these is generally the easiest and most basic way for thieves to achieve their objective. An example of **Account takeover** is when a thief gets hold of your actual physical credit card, or perhaps just the card number and expiry date, using it to purchase services or products. This works out extremely well for the thief, as the credit card owner doesn't usually notice the additional purchases until they either receive their monthly statement in the mail or have attempted to use the card and found that it has reached the maximum limit allowed.

The second type of identity theft is called **Application fraud**, or what is otherwise known as "true name fraud". In order for a thief to be successful at application fraud, they must have access to a good deal of your personal information such as your Social Security Number (SSN), full name, address, place of work, salary, driver's license number, date of birth etc. Of course not all of these pieces of information would be necessary for a thief to get away with application fraud but certainly a combination of some of the above would be required.

It Can Affect Anyone

Like many, you may assume that identity theft only happens to those people who might be a bit more careless when it comes to safeguarding personal information. Or perhaps you are of the mindset that because you don't really have a lot of money in your personal account or don't have credit cards with large spending limits, that

identity theft thieves wouldn't necessarily target someone like yourself. Well, make no mistake about it; identity theft can happen to anyone, including you! Basically, if you have an identity (and we hope that you do) then you are susceptible.

The size of your financial worth does not matter, nor whether you rent or own your home, nor whether you have exceptional credit or bad. The fact is still this, if you are reading this right now then you have an identity and because of which you are certain to have one, if not many of the following: a name, a bank account, a credit card, a telephone, a SSN, a job, a birth date, an email and internet account, a mailbox, an address, and the list goes on and on. And I hate to break this to you my friend but here's my point, it only takes one of the above pieces of information to fall into the wrong hands and you too, like millions of others can become a victim of identity theft.

Not As Difficult As You Think

Still think it's not that easy for someone to get your personal information? Well let's not be naïve about this, it's not as difficult as you think it is. Take a moment to think about all of the companies, organizations, businesses and online sites that might have access to ANY of your personal information. Think about all of the people whose hands your mail at home or at work must pass through before it reaches its intended destination.

Think about all of that extremely personal information you include on your resume when you're job hunting and that you will send it out to who knows how many companies? Your complete work history, name, contact information and possibly references are all included in your resume! What about where you work now? They have access to more of your personal information than even what your spouse or parents might have! Now think about all of the people who your employer passes that information onto, such as the insurance company, and not only your own bank but their bank as well, and let's not forget the company that processes payroll! The list is endless and in just a little while we will discuss all the ways in which you can protect yourself against identity theft. For now however, let's take a look at all of the methods in which thieves might use to access your personal information.

How Do You Know if Your Identity's Been Stolen?

Unfortunately, the most common way people find out they are victims of identity theft is when the damage is already done.

One victim tells the account of how she found out her information had been stolen. She writes:

> *"I had been thinking about buying a cellular phone but someone beat me to the punch. This person set up an account using his name and paid two bills using my Visa/debit card number. I'm not sure how he got the number since there's only one card. I've heard a lot of theories in the last few days.*
>
> *Nextel allowed this man to set up the account using my card and never verified the information. Had they checked him out, they might have found that the owner of the Visa/debit card was a woman, and not the man starting a cellular phone account. I don't even have a*
> *cell phone! The guy took more than half my paycheck, leaving me home all weekend with very little money. Luckily, rent wasn't due."*

Yet another victim writes:

> *"On Xxxx xx,2000 - my birthday - my wallet was taken at the checkout counter at (a grocery store). Security cameras showed the checker taking my wallet, and charging nearly $500 of groceries after I left the store.*
>
> *Despite my calling the police, no charges were filed against the individual because he not "steal" the wallet from my person.*
>
> *The wallet -containing my recently renewed Drivers License, MasterCard, ATM Card, parking card, business cards (with cellular and home numbers), and college ID card (with social security number on it) - was never recovered. The head of store security and the police*
> *detective told me the that wallet was probably thrown away."*

And a third account of identity theft reads:

"On September 19, I first became aware that my identity had been stolen. I received a bill from (a department store) - for $675.55 of electronic purchases I did not make. I notified (them), and put fraud alerts at the three credit reporting agencies, and ordered copies of my credit reports.

I was dumbfounded by what I discovered: over $7,000 of charges on seven credit cards, with attempts to open 6 more.

Starting on September 9th, most accounts had been opened on the Internet. Despite the fraud alert, accounts are still being opened. An account was opened at (a furniture store) on September 22nd.

The suspect presented my driver's license - and, despite the fraud alert, the miswriting of my social security number, and obvious differences in the signature - was granted instant credit. Subsequently,
nearly $3000 in charges were made, in 6 separate instances, over a four-day period."

By the time these people discovered their identity had been stolen, their credit had already been jeopardized and perhaps even ruined. They would have to embark on the unfortunate and long journey of proving their innocence.

If you know that your personal information has been accessed or otherwise tampered with there are steps you must take to stop the thieves and try to repair the damage. It is important to stay alert to signs that your information is being used without your consent even when you don't suspect you've been a victim.

Staying alert to these signs will help you respond quickly if your identity has been stolen:

- **Unfamiliar charges or withdrawals**: Always check your bank and credit card statements and make immediate inquiries to unfamiliar charges and withdrawals.
- **Missing mail:** If your bills and other mail have gone missing a thief may have broken into your mail box or had your mail redirected to a new address.
- **Calls from Creditors:** If you are being contacted by creditors you did not do business with you need to take immediate action

to find out who has.

- **New Credit Cards :** Receiving new credit cards or bills that you didn't sign for is a danger sign that your identity may have been stolen.
- **Denial of Credit:** Unexplained refusal of credit requires investigation on your part. You need to get access to your credit report right away.

What To Do if You are a Victim of Identity Theft

If the worst has happened and you find out you have indeed been a victim of identity theft (or have reason to suspect it) you must take *immediate* action to control the damage.

Report to the Credit Bureaus

If you are a victim of identity theft you must report it immediately to one of the three major credit bureaus. You only need to call one bureau to place the fraud alert and they will forward the information to the other two. Your SSN will be flagged for 90 days to prevent a thief from trying to obtain new credit with your identification.

If you are certain that your identity has been stolen you can request an extended fraud alert. The extended fraud alert will remain on your report for seven years and will require you to submit an identity theft police report.

Flagging your account will alert potential creditors to take steps to protect you. This will also delay the credit approval process.
The three bureaus are:

- **Equifax:** 1-800-525-6285
  www.equifax.com
  P.O. Box 740241, Atlanta, GA 30374-0241

- **TransUnion:** 1-800-680-7289
  www.transunion.com
  Fraud Victim Assistance Division,
  P.O. Box 6790, Fullerton, CA 92834-6790

- **Experian:** 1-888-EXPERIAN (397-3742)
  www.experian.com
  P.O. Box 9532, Allen, TX 75013

You will be asked for your SSN and other identifying information through an automated service. The alert will be passed on to the other two bureaus and all three credit bureaus will send you a letter to confirm the fraud alert is in place. You will also be given directions for

obtaining your credit report for free from each of the bureaus.

The credit reports will have a telephone number listed on them if you need to contact the bureaus about fraudulent activity listed on the reports.

Contact Your Financial Institutions and Credit Companies

Let all of your financial institutions and companies that give you credit (lines of credit, credit cards, etc.) know that you are (or might be) a victim of identity theft. Change all of your access codes - online passwords, PINs for ATMs, etc.

For NEW Accounts created by the thief: Call the creditors (including credit cards, department stores and cell phone accounts) and ask for their security or fraud department. Tell them you are an identity theft victim and ask them to close the accounts and report the closing to the credit bureau. If the account has already been used by the thief ask them not to hold you responsible for the debt.

For EXISTING Accounts used fraudulently by a thief: Close the accounts and ask the creditors to report the closing to the credit bureaus. Request that they declare the account "closed at consumer's request". If you open a new account don't use personal information like your mother's maiden name or your SSN for a password. If those are the only options request to use a different password.

Ask each company if they have a specific identity theft affidavit or theft reporting form that you should fill out.

Contact the Federal Trade Commission

Contact the Federal Trade Commission (FTC) who will assist you as a victim by providing information that will help you to resolve any financial issues or other problems as a result of your identity theft. Provide a printed copy of your FTC ID Theft Complaint to your local police department and have them include it in your report. This can provide additional protections down the road such as:

- Permanently blocking fraudulent information from appearing on your credit report.
- Keeping debts off of your credit report.

- Preventing companies from coming after you for debts that the identity thief incurred in your name.
- Keeping a longer-than-normal fraud alert on your credit report.

File a Local Police Report

Keep records of the fraudulent activity as proof for your report. Blackout unrelated activity and give copies to the police. Give them any new evidence as it turns up and keep a copy of the report as proof for creditors and the credit bureaus.

Get Copies of Your Credit Report

Send for your credit reports following the instructions from the credit bureaus. Review the reports carefully. Look for creditor's names that you did not request credit from. Also check your personal information; SSN, address, name, initials and employer information.

Order your credit report at least every three months for the first year of the fraud. Some areas provide a free report every 12 months. Other areas will give you several free reports for the year you report an identity theft. Some will charge for each report. Tell them you are an identity theft victim and ask for a free report.

Collect Account Information

Contact the creditors who issued accounts to the identity thief. The Police may give you a form to request the information. Send a copy of the police report and the account statements to the creditor. Pass any new information over to the police.

Complete an Identity Theft Affidavit

In order to remove the debts created by the identity thief you will need to send an affidavit to the company or creditor holding the debt. When you contact them to close the accounts ask what forms they require. The affidavit permits them to investigate the claim – it does not ensure that the debt will be cleared.

While each business may have its own requirements you can also obtain a free affidavit form at: http://www.ftc.gov/bcp/conline/pubs/credit/affidavit.pdf. Ask the business if they will accept this form or need you to fill out one of

theirs.

Send the copies of the affidavit and supporting documents to the businesses (a separate form should be created for each account or institution responsible for providing the identity thief with credit). Do not send original bank or card statements. Blackout any information on the statements not related to the account.

Send a copy of each affidavit and the police report to the credit bureaus. Write a letter requesting the information you declared was a result of theft be blocked or removed from your credit report.

Report Stolen Mail

If you believe that your mail has been stolen you must contact the nearest Postal Inspector. You can look for the number in your white pages under Government Services, call 1-800-ASK-USPS or search online at http://www.usps.com/ncsc/locators/find-is.html.

While the information above is provided for those living in the US the steps are nearly the same in other countries. Here are some links and numbers to credit and police agencies in the UK, Canada and Australia.

Contact Numbers for the UK

If you are a victim of identity theft in the UK use the following contact information:

Credit Bureaus

- Call Credit: 44 (0) 113 244 1555
  www.callcredit.co.uk/
  Callcredit plc, One Park Lane, Leeds.
  West Yorkshire, LS3 1EP

- Equifax: 0870 010 2091 for the CIFAS Protective Registration Service
  www.equifax.co.uk/
  Credit File Advice Centre PO Box 1140, Bradford, BD1 5US

- Experian: 0870 241 6212 (M-F 8-6, Sat 9-1)

www.experian.co.uk/
Experian Ltd, PO Box 9000, Nottingham, NG80 7WP

Police
File a report at your local Police Station. Locate the closest station at http://police.uk.

Contact Numbers for Canada

If you are a victim of identity theft in Canada use the following contact information:

Credit Bureaus

- Trans Union Canada: 1-877-525-3823 (Quebec Residents: 1-877-713-3393)
  www.tuc.ca
- Equifax Canada: 1-800-465-7166
  www.equifax.ca
  Equifax Canada Inc. Consumer Relations Department, Box 190
  Jean Talon Station, Montreal, Quebec, H1S 2Z2

Hotline

PhoneBusters National Call Centre – with a mandate to gather information and intelligence about identity theft PhoneBusters will provide advice and assistance. Toll free at 1-888-495-8501

Contact Numbers for Australia

If you are a victim of identity theft in Australia use the following contact information:

Credit Bureaus

- Baycorp Advantage: (02) 9464 6000
  www.baycorpadvantage.com
  Public Access Division
  Credit Reference Association of Australia
  PO Box 966, NORTH SYDNEY NSW 2060

- Dun and Bradstreet (Australia) Pty Ltd: 13 23 33
  www.dnb.com.au
  Attention: Public Access Centre
  PO Box 7405, St Kilda Rd VIC 3004

The Australian Crime Commission

The Australian Crime Commission operates an Identity Fraud intelligence facility that can assist victims in notifying some Australian and State government agencies that their identity has been stolen.

Tel: (02) 6243-6666

Contact your local police for instruction if the information for your country is not listed or is incorrect.

Additional Steps to Take in Recovering Your Identity and Line of Credit

- Document all of the steps that you take, names of all the people whom you deal with and any expenses you incur in re-establishing your credit and clearing your name
- Advise all of your utility companies (including home telephone and cellular service providers) that someone using your name may attempt to open unauthorized new accounts
- Contact your insurance company (homeowners/renters insurance). Some companies have coverage for losses due to theft. File a loss report if necessary.
- If you think your mail may be or has been tampered with, stolen, or someone changed your address without permission. Contact your local Postmaster or report this at www.usps.com.
- Contact your local Department of Motor Vehicles if you think someone has or is in the process of getting or renaming your drivers license or other cards.
- If you believe your Social Security Number is being used for fraudulent purposes, call their hotline at 1-800-269-0271.

- If you Passport was stolen, call the U.S. Department of State to let them know and obtain a replacement. Call them at 1-877-487-2778 or go online at http://travel.state.gov/passport
- Continue to monitor all of your bank and credit accounts on a monthly basis to make sure no further unauthorized activity is taking place.

Correcting Your Credit Report

Your credit report contains information about where you live, how you pay your bills, and whether you've been sued, arrested, or filed for bankruptcy.

Consumer reporting companies sell the information in your report to creditors, insurers, employers, and other businesses that use it to evaluate your applications for credit, insurance, employment, or renting a home. The federal Fair Credit Reporting Act (FCRA) promotes the accuracy and privacy of information in the files of the nation's consumer reporting companies.

In the case of identity theft and/or fraud, this step is essential in re-gaining your identity.

Under the FCRA, both the consumer reporting company and the information provider (that is, the person, company, or organization that provides information about you to a consumer reporting company) are responsible for correcting inaccurate or incomplete information in your report. To take advantage of all your rights under this law, contact the consumer reporting company and the information provider.

Tell the consumer reporting company, in writing, what information you think is inaccurate. Include copies (NOT originals) of documents that support your position. This would include a copy of the police report you have filed.

In addition to providing your complete name and address, your letter should clearly identify each item in your report you dispute, state the facts and explain why you dispute the information, and request that it be removed or corrected. You may want to enclose a copy of your report with the items in question circled. Send your letter by certified mail, "return receipt requested," so you can document what the

consumer reporting company received. Keep copies of your dispute letter and enclosures.

Consumer reporting companies must investigate the items in question—usually within 30 days—unless they consider your dispute frivolous. They also must forward all the relevant data you provide about the inaccuracy to the organization that provided the information.

After the information provider receives notice of a dispute from the consumer reporting company, it must investigate, review the relevant information, and report the results back to the consumer reporting company. If the information provider finds the disputed information is inaccurate, it must notify all three nationwide consumer reporting companies so they can correct the information in your file.

When the investigation is complete, the consumer reporting company must give you the results in writing and a free copy of your report if the dispute results in a change. This free report does not count as your annual free report.

If an item is changed or deleted, the consumer reporting company cannot put the disputed information back in your file unless the information provider verifies that it is accurate and complete. The consumer reporting company also must send you written notice that includes the name, address, and phone number of the information provider.

If you ask, the consumer reporting company must send notices of any corrections to anyone who received your report in the past six months. You can have a corrected copy of your report sent to anyone who received a copy during the past two years for employment purposes.

If an investigation doesn't resolve your dispute with the consumer reporting company, you can ask that a statement of the dispute be included in your file and in future reports. You also can ask the consumer reporting company to provide your statement to anyone who received a copy of your report in the recent past. You can expect to pay a fee for this service.

You should also tell the creditor or other information provider, in writing, that you dispute an item. Be sure to include copies (NOT

originals) of documents that support your position. Many providers specify an address for disputes.

If the provider reports the item to a consumer reporting company, it must include a notice of your dispute. And if you are correct—that is, if the information is found to be inaccurate—the information provider may not report it again.

YOUR LIABILITY AS THE VICTIM OF ID THEFT

The question you have probably been asking yourself throughout this entire book is…"What is my liability in this situation?" Unfortunately, that answer is fairly complex and is dependant on the type of identity theft that has occurred, as well as the timeliness in which you have responded and taken action to correct the problem. In some cases, victims are able to identify and act on the problem quickly resulting in very minimal financial loss. Other particular situations have not worked out quite so well and have resulted in substantial financial debt and a very poor credit rating, which can take years and years to repair.

Here are a few specific cases of identity theft in where the victim truly ended up as the injured party in more ways than one.

Actual Identity Theft Victim Cases

A gentleman in San Diego, California (we'll call him John Jones), encountered an identity thief who opened a PayPal account under John's name and filtered $7,600 from John's Bank of America account into the forged PayPal account. The incident occurred during July and August of 2002 but because John had been traveling he did not notice the money was actually missing until January of 2003. He contacted his bank and was informed that because he had failed to notify the bank within 60 days of the occurrence there was nothing they could do for him. By that time all of the money, with the exception of $2,100 still remaining in the PayPal account had been spent. PayPal returned the remaining sum to John but he was still out $5,000. John sued both PayPal and Bank of America in small claims court, pleading that PayPal should have notified him immediately upon discovering the fraud. Bank of America counter argued that it is the customer's responsibility to regularly check bank statements and ensure their accuracy. In the end John walked away with a settlement from each of the firms, however was still out approximately $500 as a result. His yearlong battle to turn things right was extensive, time consuming and frustrating.

An elderly woman in Seattle, Washington (we'll call her Jane Doe), was the victim of a telemarketing scam in December of last year. Jane provided her checking account information to the caller and later found

that her account had been cleaned of $800, leaving her overdrawn by $300. When her December Social Security check was deposited the Bank of America withdrew $300 of it to cover the overdraft. Jane was left with barely enough money for food and rent and was forced to "skip" Christmas that year. By February the Bank of America had returned some of the money to her and was continuing to work with her to repair the situation.

A retired California couple (let's call them the Smiths), were also the victims of identity theft in April of 2001. The Smiths, when attempting to refinance their home mortgage discovered that there was $75,000 in unsettled debts on an account that they had held with this particular mortgage company over a year ago. This was very strange, as they knew they had settled their debt and closed that account a year earlier. It seems that an identity thief had re-opened the account and switched the original mailing address to one in Houston Texas, which is why the Smiths had never received any bills or statements for that account. After three months of phone calls and paperwork, the Smiths had finally received confirmation from the mortgage company that they were not being held responsible for the debt. However, in December of 2003 the Smiths received a notice from the mortgage company's Financial Services Network that they were being sued for $75,000 plus attorney's fees for their negligence in not discovering and reporting the identity theft in a timely manner, and thus causing injury to the mortgage company. The Smiths hired a lawyer who specialized in identity theft cases and who was eventually successful in convincing the company to drop the lawsuit. The remaining bad news in this case is that the lawsuit was dropped "without prejudice", meaning that the firm could resurrect the case in the future should they choose to do so. The Smiths endured this nightmare for almost a three-year period and still the possibility of future incidents hang over their head.

This last case that I want to share with you is more than horrific but thankfully took place prior to the United States Congress making the act of Identity Theft a federal crime. Although this is certainly not something that this victim is thankful for in anyway, but we can take comfort in knowing that an incident like this would result in a very different ending in today's times. In this particular situation the criminal who was already a convicted felon accumulated more than $100,000 in credit card debt, applied for and obtained a federal home loan, bought homes, motorcycles and handguns in the victims name. The criminal went so far as to even calling the victim and taunting him

with the fact that because identity theft was not a federal crime he could continue his charade for as long as he wanted to and nothing would happen. The criminal eventually filed for bankruptcy in the victim's name while in the meantime the victim spent over $15,000 and four years in efforts to clear his name and re-establish his credit. In the end the criminal was not reprimanded in any way and never paid back one cent to the victim. His only punishment was serving a brief sentence due to the fact that he made a false statement when he purchased his firearm.

Credit Card Liability

From our research, if you have been the victim of credit card identity theft you may take some comfort in the fact that credit card liability is limited to $50. If you actually report the credit card lost prior to it being used then you cannot be held accountable for any unauthorized charges that occur after that time. However, if the identity thief uses your card before you have reported it missing or stolen then the maximum amount you will be charged is $50. The same rule applies even if the credit card is used at an ATM to withdraw cash.

Beware of telemarketers who call to sell you "loss protection" insurance for your credit cards. These callers may trick you into believing that should your card be lost or stolen that you will be solely responsible for any charges made to it if you do not have the "loss protection". Make sure to double-check that this standard still applies to your current credit cards.

ATM and Debit Card Liability

Unfortunately ATM and debit cards do not offer nearly the amount of protection that credit cards do in cases of loss or theft. It is in cases like these where time is truly of the essence and in the end it is very beneficial for you to keep proper track of your statements and card usage. When and if you do notice a discrepancy it is in your best interest to report it immediately to the issuing office. If you are fortunate in that you report the missing card prior to it being used then your financial institution cannot hold you liable for any unauthorized use. If you report the incident within two business days of the loss your liability is capped at $50. In cases where the report is made anywhere after two business days and before sixty days you will

be held liable for up to $500 of what the identity thief stole from you. If a victim were to wait more than sixty days, they could potentially lose every single cent that was stolen prior to reporting the card missing. However, we know for a fact that this last scenario couldn't possibly happen to you.

Check Liability

In most cases you would not be held liable in the situation of forged checks as the majority of States hold the bank liable. However, this doesn't mean that you have no responsibility in the situation. If you are negligent in notifying the bank within a reasonable amount of time that a check had been lost or stolen, or if you fail to monitor your account for unauthorized transactions then the liability may well rest with you.

It's Your Responsibility

Don't fool yourself into believing that when or if identity theft hits you that the responsibility lies with someone else. It certainly may not be your fault when it happens but you will be held accountable if you allow it to continue and just assume that someone else will look after the mess. It's your responsibility to protect your financial fate, security and credit rating. If you don't do it, no one else will and you will surely be taken advantage of. Take precautions, monitor your accounts and act quickly if identity theft does occur. A prompt and efficient response to the matter is the best way for you to minimize your loss.

Liability Agreements

How often do you sign up for new services, credit cards, loans or accounts? Now, how many times you actually read through the entire liability agreement that accompanies that card or service? Like most of us you may not take the time to read through those seemingly endless agreements that are filled with so much technical and legal language that it just makes your head hurt.

And what about those online agreements? Do you generally scroll down to the bottom of them without reading a word, click the "I agree" button and then hit "continue"? Many of us do and unfortunately this is where we run into trouble later on once we have become an identity thief victim. I understand that at the time it may seem tedious and unnecessary to read through those agreements but perhaps in the future you might give it a second thought. Additionally, how familiar are you with your liability responsibilities in regards to your current bank accounts, credit cards, debit cards, telephone and cellular service providers, utility providers and online PayPal, eBay and other similar accounts? This might be the perfect opportunity to go back and look at those agreements once again. You may decide that having some of those particular accounts are not worth the price you may have to pay should you one day find yourself in unfortunate circumstances such as those that our three case studies did. Hopefully though as a result of your research you are able to determine that the financial institutions and various companies that you deal with place you as their customer, on the top of their priority list ensuring that you are well protected against identity theft incidences.

CONCLUSION

Much has been covered on the topic of identity theft throughout this book and hopefully it has been successful in answering all of your questions, clarifying any misconceptions or myths and in providing you with an enlightened understanding of the issues involved in identity theft.

We have conquered not only what identity theft is and how it occurs but also, how you can have a hand in preventing it and knowing what to do when or if it does affect you. The sad reality remains however that no matter how many precautions you take it is never possible to be fully immune to identity thieves.

Even when you've done everything possible the threat still exists and always will. The best that you can do for yourself and your family is to protect what you are capable of protecting and arm yourself with the knowledge that will help you deal with whatever else it happens to be that may come along at some later point in life. Often you are not only relying on just your own actions and methods of protection but also those of the companies whom you have entrusted with your personal information.

It's very similar to when a parent tells their son or daughter who has just received their driver's license that they need to be careful on the road. The child generally responds with, "Mom, dad, I am a safe driver, don't worry about me". The parent then tells the child, "It's not your driving that I'm worried about, it's the other people on the road that concern me." The fact is, you just can't control the actions, mistakes or oversights of others. You are forced to put your faith into them and into their capabilities. You must trust that they are as concerned about your privacy and in protecting it as you are. You must believe that they will act with due diligence in taking every step possible on your behalf to prevent an act of identity theft against you. However, sometimes those people fail, they let us down and they put us at great risk.

Here are some actual headlines from major news sources of cases where very well known and very large institutions have compromised the privacy of their customers.

- *"ChoicePoint: More ID theft warnings…company says criminals able to obtain almost 140,000 names, addresses and other information."*
  Source – CNN February 2005
- *"American Online has confirmed that hackers have illegally compromised an undisclosed number of its member accounts"*
  Source – News.com June 2000
- *"LexisNexis, a worldwide provider of legal and business data, announced yesterday that information about 32,000 consumers was fraudulently gathered in a series of incidents."*
  Source – Washington Post March 2005
- *"For the second time in about a year, the credit reporting company Equifax Canada Inc. has suffered a security breach that has given criminals access to personal financial information."*
  Source – Globe And Mail June 2005
- *"AOL breach gives spam fight a twist…The security breach, believed to be one of the worst of its kind, is the latest twist in the proliferation of spam: a rogue employee supplying a subscriber list for profit."*
  Source – USA Today June 2004
- *"Bank of America says at least 1.2 million federal employee credit card accounts may be exposed to theft or hacking"*
  Source – Time February 2005

Make an effort to be familiar with those businesses that you deal with and ask them what steps and measures they take in protecting you? You have entrusted them with your personal information and financial matters, which means you have every right to expect nothing less than all of their efforts in protecting your privacy.

You also have every right to hold them accountable for any breach of privacy that does occur. Remember, these are the same companies that are telling you to protect yourself from identity theft. But are they taking the same care when it comes to your protection? You deserve to know, so ask them. There are many competing companies out there that would love your business, and if the ones that you are working with currently can't satisfy you with the kinds of answers that these important questions deserve, be confident and know that someone in some other place certainly can.

RESOURCES

Use the following list of resources to help you in taking action if you have become an identity theft victim.

Credit Card Contact Information
Visa – (800) 847-2911
Mastercard – (800) 622-7747
American Express – (800) 554-2639

Credit Bureau Fraud Departments
TransUnion
Fraud Victim Assistance Department
Phone: (800) 680-7289
Fax: (714) 447-6034
P.O. Box 6790
Fullerton, CA 92634-6790

Equifax
Consumer Fraud Division
Phone: (800) 525-6285 or (404) 885-8000
Fax: (770) 375-2821
P.O. Box 740241
Atlanta, GA 30374-0241

Experian
Experian's National Consumer Assistance
Phone: (888) 397-3742
P.O. Box 2104
Allen, TX 75013

Check Verification Companies
Check Rite – (800) 766-2748
Chex Systems – (800) 328-5121
CrossCheck – (800) 552-1900
Equifax-Telecredit – (800) 437-5120
NPC – (800) 526-5380
SCAN – (800) 262-7771
Tele-Check – (800) 366-2425

REFERENCES

- Identity Theft Resource Center www.idtheftcenter.org
- Federal Trade Commission http://www.ftc.gov/index.html
- Bankrate www.bankrate.com
- Chicago Better Business Bureau http://www.chicago.bbb.org/idtheft/typesof.html
- Office of the Privacy Commissioner of Canada http://www.privcom.gc.ca/index_e.asp
- MSNBC http://msnbc.msn.com/id/4264051
- Privacy Rights Clearing House http://www.privacyrights.org/index.htm
- Fight Identity Theft www.fightidentitytheft.com
- Protect My Info http://what-is-identity-theft.com
- Computer World http://www.computerworld.com
- All Free Info.com http://all-free-info.com/phishing
- United States Department of Justice http://www.usdoj.gov/index.html